2階算術における実数と複素数 (圏論と証明論の新たな融合を目指して)

AUTHOR(S):

坂本, 伸幸; 田中, 一之

CITATION:

坂本, 伸幸 ...[et al]. 2階算術における実数と複素数 (圏論と証明論の新たな融合を目指して). 数理解析研究所講究録 2001, 1217: 98-120

ISSUE DATE:

2001-06

URL:

http://hdl.handle.net/2433/41235

数理解析研究所講究録 1217 巻 2001 年 98-120

2階算術における実数と複素数

東北大学大学院理学研究科数学専攻
坂本 伸幸 (SAKAMOTO, Nobuyuki)
田中 一之 (TANAKA, Kazuyuki)

概 要

本論文は，RCA_0 における実数，複素数の取り扱い，特に，シンプソン・田中・山崎のメタ定理 [6] に関連する話題を中心としたものである．この定理は，実閉体（代数閉体）の理論の定理が RCA_0 における実数（複素数）に関して成り立つことを主張するものである．第1節では2階算術，逆数学の基礎の概説をおこなう．第2節では，RCA_0 において実数の集まりが実閉体になるという定理を紹介する．実は，この定理の強化版がまだ未解決であるのだが，解決の足がかりとして，条件を弱めることによって強化版の部分的解決を試みる．また，この定理とも密接に関係する，代数学の強基本定理を RCA_0 で証明する．これは，定数でない複素係数多項式の重複を込めた根全体の存在を主張する定理である．第3節では，より強い集合存在公理を必要とする実数の性質を見る．また，上の未解決問題がより強い集合存在公理を仮定すれば証明可能であることを見る．

1 2階算術と実数

2階算術とは，自然数と自然数からなる集合を対象とした理論である．この理論がほぼ数学全般の土台になりうることはかなり昔から知られている．例えば，有理数の可算列を考えることによって実数を取り扱うことができ，実数の可算列を考えることによって実数から実数への連続関数を扱える．

この理論を用いて，個々の数学の定理の証明に必要な公理は何かを調べようというのが「逆数学」である．より詳しく言えば，逆数学とは，RCA_0 という体系をもとにして，ある数学の定理の証明に必要十分な集合存在公理を求めようというプログラムである．

本節では，実数の議論に必要な2階算術の基礎知識について説明する．

1.1 2階算術

まず，2階算術の説明を簡単に行う．2階算術の詳細については [5] を参照.

定義 1.1.1 ($\mathcal{L}_2$). **2階算術の言語$\mathcal{L}_2$**は，数変数 $x, y, z, \ldots$ と集合変数 $X, Y, Z, \ldots$ を持つ2領域言語である．数項は数変数と定数記号 $0, 1$ から加法，乗法によって得られるものとし，原子論理式は数項 s, t，集合変数 X によって $s = t, s < t, s \in X$ と表されるものとする．論理式は原子論理式から命題結合記号 $\neg, \wedge, \vee, \rightarrow$ と量化記号 $\forall, \exists$ を用いて構成される.

定義 1.1.2 (論理式の階層). **量化記号のない論理式 (quantifier free formula, q.f. formula)** とは，量化記号 $(\forall, \exists)$ を含まない論理式のこととする．Σ^0_0 **論理式**とは，含まれる量化記号がすべて $\forall x < t, \exists x < t$ (x は数変数，t は x を含まない数項) の形である論理式のこととする．Σ^0_0 論理式のことを Π^0_0 **論理式**，Δ^0_0 **論理式**とも呼ぶ．Σ^0_{n+1} **論理式**とは，ある Π^0_n 論理式 $\varphi(x)$ があって，

$$\exists x \varphi(x)$$

と書けるものとする．ただし，$\varphi(x)$ はパラメータ（x 以外の自由変数）を含んでよい．以下同様．Π^0_{n+1} **論理式**とは，ある Σ^0_n 論理式 $\varphi(x)$ があって，

$$\forall x \varphi(x)$$

と書けるものとする．Σ^1_0 **論理式**とは，ある自然数 n に対して Σ^0_n 論理式となる論理式のこととする．Σ^1_0 論理式のことを Π^1_0 **論理式**，Δ^1_0 **論理式**とも呼ぶ．Σ^1_{n+1} **論理式**とは，ある Π^1_n 論理式 $\varphi(X)$ があって，

$$\exists X \varphi(X)$$

と書けるものとする．Π^1_{n+1} **論理式**とは，ある Σ^1_n 論理式 $\varphi(X)$ があって，

$$\forall X \varphi(X)$$

と書けるものとする．$i = 0, 1, j = 0, 1, \ldots$ に対し，Σ^i_j 論理式，Π^i_j 論理式全体の集合をそれぞれ Σ^i_j，Π^i_j で表す．関係が Δ^i_j であるとは，この関係が Σ^i_j 論理式でも Π^i_j 論理式でも記述できる[1]ことを言う.

[1] 正確には，考える体系に依存している

定義 1.1.3 ($\Sigma^0_0(\Gamma)$)**.** Γ を論理式の集合とする．Γ に属する論理式を命題結合記号，有限量化記号によって結合してできる論理式全体を $\Sigma^0_0(\Gamma)$ で表す．$\Sigma^0_0(\Gamma)$ に属する論理式を $\Sigma^0_0(\Gamma)$ **論理式**と呼ぶ．

定義 1.1.4 (帰納法と有界内包公理). Γ を論理式の集合とする．次の 4 つの公理図式を定義する．

$$\begin{aligned}
\Gamma\text{-IND}\,(\Gamma\text{ 帰納法}) &: [\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x+1))] \to \forall x\varphi(x)\\
\Gamma\text{-CA}\,(\Gamma\text{ 内包公理}) &: \exists X\forall i(i \in X \leftrightarrow \psi(i))\\
\Gamma\text{-BCA}\,(\text{有界}\Gamma\text{ 内包公理}) &: \forall n\exists X\forall i(i \in X \leftrightarrow (i < n \wedge \psi(i)))\\
\Gamma\text{-LNP}\,(\Gamma\text{ 最小値原理}) &: \exists x\varphi(x) \to \exists x[\varphi(x) \wedge \forall y < x\neg\varphi(y)]
\end{aligned}$$

ここに，$\varphi, \psi \in \Gamma$ で，ψ は X を自由変数として含まない．

定義 1.1.5 (RCA_0)**.** RCA_0 は言語 $\mathcal{L}_2$ を持つ体系で，公理として $(\omega, +, \cdot, 0, 1, <)$ に関する離散順序半環の公理（ここに，ω は自然数全体の集合を表す）と Σ^0_1-IND と Δ^0_1 内包公理

$$\forall n(\varphi(n) \leftrightarrow \psi(n)) \to \exists X\forall n(n \in X \leftrightarrow \varphi(n))$$

（φ は Σ^0_1 論理式，ψ は Π^0_1 論理式で X が自由に現れない）を持つ体系とする．

RCA_0 において，2 個の自然数のペアを 1 個の自然数によってコード化できる．ペア i, j のコードを $\langle i, j\rangle$ とする．また，自然数の有限列もコード化できる．有限列 $s_0, s_1, \ldots, s_n$ のコードを $\langle s_0, s_1, \ldots, s_n\rangle$ で表す．有限列のコード全体を Seq で表し，特に 0, 1 だけからなる有限列のコード全体を Seq_2 で表す．以降，有限列とそのコードを同一視する．$s^\frown t$ で有限列 s, t の結合を表し，$(s)_i$ で有限列 s の $i+1$ 番目の要素を表す．すなわち，

$$s = \langle s_0, s_1, \ldots, s_n\rangle$$

であるとき，$(s)_i = s_i$ である．また，$\mathrm{lh}(s)$ で有限列 s の長さを表し，$i \le \mathrm{lh}(s)$ に対し，$s[i]$ で $\langle (s)_0, (s)_1, \ldots, (s)_{i-1}\rangle$ を表すことにする．$\mathrm{lh}(s) = n, (s)_i = n, s^\frown t = u$ などの関係は Σ^0_0 論理式で表現できる．また，自然数の有限列のコード化は

$$\forall i \le n(s_i \le s'_i) \Rightarrow \langle s_0, s_1, \ldots, s_n\rangle \le \langle s'_0, s'_1, \ldots, s'_n\rangle$$

を成り立たせているとしてよい.

集合 f が Y から Z への**関数**であるとは，f は Y の元 y と Z の元 z のペア $\langle y,z\rangle$ たちからなり，

$$\forall y \in Y \exists z \in Z(\langle y,z\rangle \in f)$$
$$\forall x \forall y \forall y'(\langle x,y\rangle \in f \wedge \langle x,y'\rangle \in f \to y = y')$$

を満たすことをいう．関数については，関数合成が自然にでき，ゼロ関数 $\lambda x.0$，後継者関数 $\lambda x.x+1$，射影関数 $\lambda x_0 x_1 \ldots x_i.x_j$ $(0 \leq j \leq i)$ が存在すること，関数のクラスが原始再帰法，最小化演算について閉じていることを RCA_0 で証明できることが知られている．詳しくは [5] を参照のこと.

以下では，論理式の集合 Γ に対し,「論理式 φ がある論理式 $\psi \in \Gamma$ と RCA_0 で同値」であることを，単に「φ は Γ である」と略記する.

φ, ψ が Σ^0_k ならば，$\varphi \wedge \psi, \varphi \vee \psi, \exists x < u\varphi$ も Σ^0_k であることはよく知られている．さらに，次のこともいえる.

定理 1.1.6. k を自然数とし，$\varphi \in \Pi^0_k$ とする．$\mathsf{RCA}_0 + \Sigma^0_{k+1}$-IND において

$$\forall x < v \exists y \varphi(x,y) \to \exists u \forall x < v \exists y < u \varphi(x,y)$$

が示せ，$\forall x < v \exists y \varphi(x,y)$ はある Σ^0_{k+1} 論理式と（$\mathsf{RCA}_0 + \Sigma^0_{k+1}$-IND で）同値になる.

証明 k に関する帰納法で証明する.

$k = 0$ の場合を示す．$\forall x < a \exists y \varphi(x,y)$ を仮定する．$\psi(v) \equiv \exists s \forall x < v \exists y < s \varphi(x,y) \vee a < v$ とおく．これは Σ^0_1 論理式で，$\psi(0)$ と $\psi(v) \to \psi(v+1)$ がいえるから，Σ^0_1-IND により $\forall v \psi(v)$．特に $\psi(a)$，すなわち $\exists s \forall x < a \exists y < s \varphi(x,y)$．$\exists u \forall x < v \exists y < u \varphi(x,y) \to \forall x < v \exists y \varphi(x,y)$ は明らかだから，$\forall x < v \exists y \varphi(x,y)$ は Σ^0_1 論理式 $\exists u \forall x < v \exists y < u \varphi(x,y)$ と同値である.

$k > 0$ とする．前と同じように，$\forall x < a \exists y \varphi(x,y)$ を仮定し，$\psi(v) \equiv \exists s \forall x < v \exists y < s \varphi(x,y) \vee a < v$ とおく．ここに，$\exists y < s \varphi(x,y) \leftrightarrow \neg(\forall y < s \neg\varphi(x,y))$ だから，帰納法の仮定により ψ はある Σ^0_{k+1} 論理式と同値．以降は $k = 0$ の場合と同様である．□

帰納法，有界内包公理，最小値原理については次のことが知られている.

定理 1.1.7 (帰納法，有界内包公理，最小値原理の同値性). 任意の k に対して，RCA_0 において Σ^0_k-IND, $\Sigma^0_0(\Sigma^0_k)$-IND, Σ^0_k-LNP, $\Sigma^0_0(\Sigma^0_k)$-LNP, Σ^0_k-BCA, $\Sigma^0_0(\Sigma^0_k)$-BCA は同値で

ここで，逆数学プログラムで用いられる体系のうち，本論文に関係するものを紹介する．

定義 1.1.8 (WKL_0, ACA_0). RCA_0 に“任意の無限2分木（$\subseteq \mathrm{Seq}_2$）は無限道をもつ”ことを表す公理図式を加えた体系を WKL_0 とする．RCA_0 に公理図式 Σ^1_0-CA を加えた体系を ACA_0 とする．

1.2 2階算術における数の取り扱い

RCA_0 における自然数全体の集合，すなわち $x \in X \leftrightarrow x = x$ なる集合 X を $\mathbb{N}$ で表す．整数，有理数は自然数で容易に表現できる．整数は自然数のペアを適当な同値関係で類別したものの代表元全体，有理数は整数のペアを適当な同値関係で類別したものの代表元全体とすればよい．整数全体，有理数全体の集合をそれぞれ $\mathbb{Z}, \mathbb{Q}$ で表す．しかし，実数，複素数の取り扱いは簡単ではない．

定義 1.2.1 (実数，複素数). RCA_0 において，実数は，有理数の無限列 $\langle q_k : k \in \mathbb{N} \rangle$ で，

$$\forall k \forall i (|q_k - q_{k+i}| \leq 2^{-k})$$

を満たすものとする．二つの実数 $x = \langle q_k : k \in \mathbb{N} \rangle, y = \langle q'_k : k \in \mathbb{N} \rangle$ の和，積や x のマイナス元が

$$x + y = \langle q_{k+1} + q'_{k+1} : k \in \mathbb{N} \rangle$$
$$xy = \langle q_{k+m} + q'_{k+m} : k \in \mathbb{N} \rangle$$
$$-x = \langle -q_k : k \in \mathbb{N} \rangle$$

（ここに，m は $\max(|q_0|, |q'_0|) + 1 \leq 2^{m-1}$ となる最小の自然数）で定められる．一般に，多変数多項式 t，実数 $x_0, x_1, \ldots, x_n$ に対し，実数 $t(x_0, x_1, \ldots, x_n)$ の各成分が x_i たちの成分から和，積をもちいて得られる．また，二つの実数 x, y に対し，

$$y(x/y) = x \ \ (y \neq 0), \quad x/0 = 0$$

を成り立たせる x/y が存在することがわかる（命題1.2.4参照）．

二つの実数 $x = \langle q_k : k \in \mathbb{N} \rangle, y = \langle q'_k : k \in \mathbb{N} \rangle$ に対し，

$$x \leq y \equiv \forall k (q_k \leq q'_k + 2^{-k+1})$$

と定め，$x<y\equiv\neg(y\leq x), x=y\equiv(x\leq y\wedge y\leq x)$ と定める．

複素数は，2個の実数のペア (x,y) とし，複素数 $c=(x,y), d=(x',y')$ に対し加法，マイナス元，乗法，除法を

$$c+d=(x+x',y+y')$$
$$-d=(-x',-y')$$
$$c\cdot d=(xx'-yy',xy'+x'y)$$
$$c/d=(\frac{xx'+yy'}{x^2+y^2},\frac{x'y-xy'}{x^2+y^2})$$

と定める．(x,y) は $x+y\sqrt{-1}$ を意図している．

定義 1.2.2 (無限実数列，無限複素数列). 集合 X が与えられたとき，各 $i\in\mathbb{N}$ に対し，

$$(X)_i=\{y|\langle i,y\rangle\in X\}$$

とおく（この集合は Σ^0_0-CA により存在）．E が**無限実数列**であるとは，任意の i に対し $(E)_i$ が実数であることとする．E が長さ l の**有限実数列**であるとは，任意の $i<l$ に対し $(E)_i$ が実数であることとする．無限実数列全体を（非公式に）$\mathbb{R}^{\mathbb{N}}$ と表し，長さ l の有限実数列全体を（非公式に）$\mathbb{R}^l$ と表す．**有限複素数列，無限複素数列**も同様に定め，無限複素数列全体を（非公式に）$\mathbb{C}^{\mathbb{N}}$ と表し，長さ l の有限複素数列全体を（非公式に）$\mathbb{C}^l$ と表す．

RCA_0 における実数，複素数について，次のような性質が成り立つ．

命題 1.2.3. RCA_0 で以下のことが証明できる．$n\in\mathbb{N}$ とする．長さ n 以上の任意の有限実数（複素数）列 E に対し，

$$i\in X\leftrightarrow(i<n\wedge(E)_i=0)$$

なる集合 X が存在する．

証明 関係 $(E)_i=0$ が Π^0_1 だから，Π^0_1-BCA より直ちにわかる． □

命題 1.2.4. RCA_0 で以下のことが証明できる．$n\in\mathbb{N}$ とする．長さ n 以上の有限実数（複素数）列 E に対し，長さ n の有限実数（複素数）列 F で，$(F)_i=1/(E)_i$ なるものが存在する．

証明 まず実数の場合を示す．前命題より，$i \in X \leftrightarrow (i < n \wedge (E)_i = 0)$ なる集合 X がとれる．最小化演算を用いて，長さ n の自然数の有限列 s で，$i \notin X$ のとき，$(s)_i$ は

$$|((E)_i)_m| > 2^{-m+1}$$

をみたす最小の m であるようなものがとれる．このとき，実数の定義から，任意の $j \in \mathbf{N}$ に対し

$$|((E)_i)_{(s)_i+j}| \geq 2^{-(s)_i+1} - 2^{-(s)_i} = 2^{-(s)_i}$$

が成立する．F を次のように定める．$i \in X$ ならば $((F)_i)_k = 0$ とし，$i \notin X$ ならば $((F)_i)_k = 1/((E)_i)_{k+2(s)_i}$ とする．前者の場合 $(F)_i = 0$ で，後者の場合，任意の $j \in \mathbf{N}$ に対し，

$$\begin{aligned} |((F)_i)_k - ((F)_i)_{k+j}| &= \left| \frac{1}{((E)_i)_{k+2(s)_i}} - \frac{1}{((E)_i)_{k+j+2(s)_i}} \right| \\ &= \frac{|((E)_i)_{k+2(s)_i} - ((E)_i)_{k+j+2(s)_i}|}{((E)_i)_{k+2(s)_i}((E)_i)_{k+j+2(s)_i}} \\ &\leq \frac{2^{-k-2(s)_i}}{2^{-(s)_i} \cdot 2^{-(s)_i}} \\ &= 2^{-k} \end{aligned}$$

だから $(F)_i$ は実数．これが $(F)_i = 1/(E)_i$ を満たすことも

$$\langle ((E)_i)_k : k \in \mathbf{N} \rangle = \langle ((E)_i)_{k+2(s)_i} : k \in \mathbf{N} \rangle$$

（両辺は実数として等しい）からわかる．複素数の場合は $1/(x + y\sqrt{-1}) = (x - y\sqrt{-1})/(x^2 + y^2)$ から示せる． □

2 実数，複素数の計算と充足論理式

RCA_0 で実数，複素数の計算を行おうとすると大変面倒な議論が必要となる．この手間を軽減できるメタ定理が [6] で証明された．この結果は，実閉体のすべての定理は $\mathbf{R}$ において成り立つということを主張するものである．この定理を結果のみ紹介する．また，この結果をより強いものに置き換えることができるか考察する．そして，この定理の証明に必要となる代数学の基本定理の証明を見る．

2.1 実数，複素数の計算と充足論理式

定義 2.1.1 (ACF(0), RCOF). 言語 $\mathcal{L}_{\mathsf{AF}}$ は体の言語（$\langle +, -, \cdot, /, 0, 1, = \rangle$）とする．体系 AF は言語が $\mathcal{L}_{\mathsf{AF}}$ で，以下の公理を持つものとする．

$$x+0=x, \quad x+y=y+x, \quad x+(y+z)=(x+y)+z, \quad x+(-x)=0$$
$$x\cdot 0=0, \quad x\cdot 1=x, \quad x\cdot y=y\cdot x, \quad x\cdot(y\cdot z)=(x\cdot y)\cdot z$$
$$x/0=0, \quad x\neq 0 \to x\cdot(y/x)=y$$
$$1\neq 0, \quad x\cdot(y+z)=(x\cdot y)+(x\cdot z)$$

ACF(0) は AF に以下の公理を加えたものとする．

$$\overbrace{1+1+\cdots+1}^{n\text{個}}\neq 0 \quad (n\geq 2)$$
$$\forall x_0\forall x_1\cdots\forall x\exists y(x_n\neq 0 \to x_0+x_1y+\cdots+x_ny^n=0) \quad (n\geq 1)$$

これは標数0の代数的閉体の公理を表している．

言語 $\mathcal{L}_{\mathsf{OF}}$ は $\mathcal{L}_{\mathsf{AF}}$ に $<$ を加えたものとする．体系 RCOF は言語が $\mathcal{L}_{\mathsf{AF}}$ で，公理は AF に

$$< \text{は線形順序}, \quad 0<1$$
$$(x>0\wedge y>0)\to(x+y>0\wedge xy>0)$$

と

$$\forall x_0\forall x_1\cdots\forall x_n\forall y\forall z($$
$$(y<z\wedge x_0+x_1y+\cdots+x_ny^n<0<x_0+x_1z+\cdots+x_nz^n)$$
$$\Rightarrow\exists u(y<u<z\wedge x_0+x_1u+\cdots+x_nu^n=0)) \quad (n>0)$$

を加えたものとする．これは実閉順序体の公理を表している．

以下，RCA_0 で ACF(0), RCOF が形式化されているとし（項，論理式，証明が自然数にコード化されている），その際の ACF(0), RCOF の変数は $v_0, v_1, \ldots$ であるとする．また，t' を t の部分項とするとき，t' のコードは t のコードより小さいとしてお

く．さらに，ACF(0), RCOF の体系の論理式とその RCA_0 におけるコードを自然に同一視する．そして，任意の無限複素数列 E，複素数 A に対し，E^i_A で E の i 番目の複素数を A に置き換えて得られる複素数列を表すとする．無限実数列 E と実数 A に対しても同様の定義をする．

定義 2.1.2 (l 解釈列). 無限複素数列 E，自然数 l に対し，有限複素数列

$$V_E = \langle V_E(s) : s < l, s \text{ は ACF(0) の項のコード} \rangle$$

が環境 E における l 解釈列であるとは，

$$V_E(0) = 0, \quad V_E(1) = 1$$
$$V_E(v_i) = (E)_i$$
$$V_E(t_1 + t_2) = V_E(t_1) + V_E(t_2), \quad V_E(-t) = -V_E(t)$$
$$V_E(t_1 t_2) = V_E(t_1)V_E(t_2), \quad V_E(t_1/t_2) = V_E(t_1)/V_E(t_2)$$

が成り立つことをいう．有限実数列に対する l 解釈列も同様に定義する．

以下の定理は，実数，複素数に関する基本的な演算が RCA_0 でできることを主張する．

定理 2.1.3. RCA_0 で以下の主張がいえる．任意の無限複素数列 E，自然数 l に対し，l 解釈列が存在する．しかも，l 解釈列は次の意味で一意である．V_E が環境 E における l 解釈列で，$V'_{E'}$ が環境 E' における l' 解釈列であり，項 s のコードが l と l' より小さく，s に現れる自由変数を $v_{i_0}, v_{i_1}, \ldots, v_{i_j}$ とするとき，

$$(E)_{i_0} = (E')_{i_0}, (E)_{i_1} = (E')_{i_1}, \ldots, (E)_{i_j} = (E')_{i_j}$$

が成り立つならば，

$$V_E(s) = V'_{E'}(s).$$

実数に関しても同様の主張が成り立つ． □

さらに，次の充足論理式に関する結果がある．

定理 2.1.4 (充足論理式). RCA_0 の Δ^0_2 論理式 $\mathrm{SAT}_{\mathbb{C}}(x,E), \mathrm{SAT}_{\mathbb{R}}(x,E)$ で，以下の3つの主張を満たすものが存在する．

1) タルスキの充足条件．すなわち，

$$\begin{aligned}
\mathrm{SAT}_{\mathbb{R}}(t_1 = t_2, E) &\Leftrightarrow \text{ある } l \text{ 解釈列 } V_E \text{ に対し}, V_E(t_1) = V_E(t_2)\\
&\Leftrightarrow \text{任意の } l \text{ 解釈列 } V_E \text{ に対し}, V_E(t_1) = V_E(t_2)\\
\mathrm{SAT}_{\mathbb{R}}(t_1 < t_2, E) &\Leftrightarrow \text{ある } l \text{ 解釈列 } V_E \text{ に対し}, V_E(t_1) < V_E(t_2)\\
&\Leftrightarrow \text{任意の } l \text{ 解釈列 } V_E \text{ に対し}, V_E(t_1) < V_E(t_2)\\
\forall i \le n \mathrm{SAT}_{\mathbb{R}}(\varphi_i, E) &\Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\varphi_0 \wedge \varphi_1 \wedge \cdots \wedge \varphi_n, E)\\
\exists i \le n \mathrm{SAT}_{\mathbb{R}}(\varphi_i, E) &\Leftrightarrow \mathrm{SAT}_{\mathbb{R}}(\varphi_0 \vee \varphi_1 \vee \cdots \vee \varphi_n, E)\\
\neg \mathrm{SAT}_{\mathbb{R}}(\varphi, E) &\Leftrightarrow \mathrm{SAT}_{\mathbb{R}}(\neg\varphi, E)\\
\forall A \in \mathbb{R}(\mathrm{SAT}_{\mathbb{R}}(\varphi, E^i_A)) &\Leftrightarrow \mathrm{SAT}_{\mathbb{R}}(\forall v_i \varphi, E)\\
\exists A \in \mathbb{R}(\mathrm{SAT}_{\mathbb{R}}(\varphi, E^i_A)) &\Leftrightarrow \mathrm{SAT}_{\mathbb{R}}(\exists v_i \varphi, E).
\end{aligned}$$

2) 実閉体で成り立つことは任意の実数に対して成り立つ．すなわち，

$$(\mathsf{RCOF} \vdash \varphi) \Leftrightarrow \forall E \in \mathbb{R}^{\mathbb{N}} \mathrm{SAT}_{\mathbb{R}}(\varphi, E).$$

3) 任意の $E, E' \in \mathbb{R}^{\mathbb{N}}$ と φ について，各 i に対し「v_i が φ に自由に現れるならば $(E)_i = (E')_i$」となるならば

$$\mathrm{SAT}_{\mathbb{R}}(\varphi, E) \Leftrightarrow \mathrm{SAT}_{\mathbb{R}}(\varphi, E')$$

となる．

$\mathrm{SAT}_{\mathbb{C}}$ も“タルスキの充足条件”を満たし，

$$(\mathsf{ACF}(0) \vdash \varphi) \Leftrightarrow \forall E \in \mathbb{C}^{\mathbb{N}} \mathrm{SAT}_{\mathbb{C}}(\varphi, E)$$

が成立する．そして，任意の $E, E' \in \mathbb{C}^{\mathbb{N}}$ と φ について，各 i に対し「v_i が φ に自由に現れるならば $(E)_i = (E')_i$」となるならば

$$\mathrm{SAT}_{\mathbb{C}}(\varphi, E) \Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\varphi, E')$$

となる． □

注意 2.1.5 (算術に対する充足論理式). $\langle \mathbb{N}, +, \cdot, 0, 1, =, < \rangle$ に関する“タルスキの充足条件”を満たす論理式 $\mathrm{SAT}_{\mathbb{N}}$ が Σ^1_0 ではとれないが Δ^1_1 でとれることが知られている（[2, Ch.IV]，[1, Ch.C.1.] 等を参照）．

2.2 未解決問題 SSC

実は，次の問題がまだ未解決である．

予想 2.2.1. 前に定めた RCA_0 の論理式 $\mathrm{SAT}_{\mathbb{R}}$ は次のことも満たす．

$$\forall n[\mathrm{SAT}_{\mathbb{R}}(\exists v_{i_0}\exists v_{i_1}\cdots\exists v_{i_{n-1}}\varphi, E) \Rightarrow \exists A \in \mathbb{R}^n(\mathrm{SAT}_{\mathbb{R}}(\varphi, E^{i_0,i_1,\ldots,i_{n-1}}_{(A)_0,(A)_1,\ldots,(A)_{n-1}}))]$$

ただし，$E^{i_0,i_1,\ldots,i_{n-1}}_{(A)_0,(A)_1,\ldots,(A)_{n-1}}$ は，各 k に対し，E の i_k 番目を $(A)_{i_k}$ で置き換えたものを表す．

ただし，この予想の $\Rightarrow$ を $\Leftarrow$ に置き換えたものが成り立つことは [6] の証明を見ることにより容易にわかる．この問題を本論文では**SSC** (Strong Satisfaction Condition) と呼ぶことにする．この問題の複素数版もまた未解決である．この予想が解決されれば，RCA_0 における実数に関する多くの問題の取り扱いが容易になることが期待される．

しかし，論理式の形を制限すればこの問題は解決できる．以下でそのことを見よう．

命題 2.2.2. 量化記号と演算記号 $\cdot, /$ を持たない論理式 $\varphi(v,\vec{w})$ に対し，変数 v を持たない AF の項の列 $t_1(\vec{w}), t_2(\vec{w}), \ldots, t_k(\vec{w})$ が原始再帰的にとれ，

$$\mathsf{RCOF} \vdash [\exists v\varphi(v,\vec{w}) \leftrightarrow \varphi(t_1(\vec{w}),\vec{w}) \vee \varphi(t_2(\vec{w}),\vec{w}) \vee \cdots \vee \varphi(t_k(\vec{w}),\vec{w})]$$

となる．

証明 与えられた φ に対し，原子論理式を $\wedge$ でつないだ形の論理式 $\varphi_i \equiv \alpha^i_1 \wedge \alpha^i_2 \wedge \cdots \wedge \alpha^i_{l_i}$ たちが存在し，

$$\varphi(v,\vec{w}) \leftrightarrow \varphi_1(v,\vec{w}) \vee \varphi_2(v,\vec{w}) \vee \cdots \vee \varphi_l(v,\vec{w})$$

とできる．各 φ_i に対し，

$$\exists v\varphi_i(v,\vec{w}) \leftrightarrow \varphi_i(t^i_1(\vec{w}),\vec{w}) \vee \varphi_i(t^i_2(\vec{w}),\vec{w}) \vee \cdots \vee \varphi_i(t^i_{k_i}(\vec{w}),\vec{w})$$

なる項の列 $t_1^i(\vec{w}), t_2^i(\vec{w}), \ldots, t_{k_i}^i(\vec{w})$ が得られていれば，

$$\begin{aligned}
\exists v\varphi(v,\vec{w}) &\leftrightarrow \exists v\varphi_1(v,\vec{w}) \vee \exists v\varphi_2(v,\vec{w}) \vee \cdots \vee \exists v\varphi_l(v,\vec{w}) \\
&\leftrightarrow \varphi_1(t_1^1(\vec{w}),\vec{w}) \vee \varphi_1(t_2^1(\vec{w}),\vec{w}) \vee \cdots \vee \varphi_1(t_{k_1}^1(\vec{w}),\vec{w}) \\
&\vee \varphi_2(t_1^2(\vec{w}),\vec{w}) \vee \varphi_2(t_2^2(\vec{w}),\vec{w}) \vee \cdots \vee \varphi_2(t_{k_2}^2(\vec{w}),\vec{w}) \\
&\vee \cdots \\
&\vee \varphi_l(t_1^l(\vec{w}),\vec{w}) \vee \varphi_l(t_2^l(\vec{w}),\vec{w}) \vee \cdots \vee \varphi_l(t_{k_l}^l(\vec{w}),\vec{w}) \\
&\rightarrow \varphi(t_1^1(\vec{w}),\vec{w}) \vee \varphi(t_2^1(\vec{w}),\vec{w}) \vee \cdots \vee \varphi(t_{k_1}^1(\vec{w}),\vec{w}) \\
&\vee \varphi(t_1^2(\vec{w}),\vec{w}) \vee \varphi(t_2^2(\vec{w}),\vec{w}) \vee \cdots \vee \varphi(t_{k_2}^2(\vec{w}),\vec{w}) \\
&\vee \cdots \\
&\vee \varphi(t_1^l(\vec{w}),\vec{w}) \vee \varphi(t_2^l(\vec{w}),\vec{w}) \vee \cdots \vee \varphi(t_{k_l}^l(\vec{w}),\vec{w})
\end{aligned}$$

とできる．したがって，はじめから φ は原子論理式を $\wedge$ でつないだ形 $\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_k$ であるとしてよい．

項 t と正の自然数 m に対し，mt で t を m 回足しあわせたものを表すとすれば，「移項」することにより，各 α_i は $mv < t, mv = t, mv > t$ ($m \in \mathbb{N}$, t は変数 v と演算記号 $\cdot, /$ を含まない項) のいずれかの形であるとしてよい．また，ある α_j が変数 v_i を含まなければ

$$\exists v(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_k) \leftrightarrow \alpha_j \wedge \exists v(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_{j-1} \wedge \alpha_{j+1} \wedge \cdots \wedge \alpha_k)$$

である．$\varphi' \equiv \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_{j-1} \wedge \alpha_{j+1} \wedge \cdots \wedge \alpha_k$ に対し，

$$\exists v\varphi'(v,\vec{w}) \leftrightarrow \varphi'(t_1'(\vec{w}),\vec{w}) \vee \varphi'(t_2'(\vec{w}),\vec{w}) \vee \cdots \vee \varphi'(t_{k'}'(\vec{w}),\vec{w})$$

なる項の列 $t_1'(\vec{w}), t_2'(\vec{w}), \ldots, t_{k'}'(\vec{w})$ が得られているとすれば，

$$\begin{aligned}
\exists v\varphi_i(v,\vec{w}) &\leftrightarrow \alpha_j(\vec{w}) \wedge \exists v\varphi'(v,\vec{w}) \\
&\leftrightarrow \alpha_j(\vec{w}) \wedge (\varphi'(t_1'(\vec{w}),\vec{w}) \vee \varphi'(t_2'(\vec{w}),\vec{w}) \vee \cdots \vee \varphi'(t_{k'}'(\vec{w}),\vec{w})) \\
&\leftrightarrow (\alpha_j(\vec{w}) \wedge \varphi'(t_1'(\vec{w}),\vec{w})) \vee (\alpha_j(\vec{w}) \wedge \varphi'(t_2'(\vec{w}),\vec{w})) \\
&\quad \vee \cdots \vee (\alpha_j(\vec{w}) \wedge \varphi'(t_{k'}'(\vec{w}),\vec{w})) \\
&\leftrightarrow \varphi(t_1'(\vec{w}),\vec{w}) \vee \varphi(t_2'(\vec{w}),\vec{w}) \vee \cdots \vee \varphi(t_{k_i}'(\vec{w}),\vec{w})
\end{aligned}$$

となる．だから，はじめから各α_jは変数vを含むとしてよい．以上により，φは

$$\begin{aligned} & m_1 v < r_1 \wedge \cdots \wedge m_{k_0} v < r_{k_0} \\ \wedge \quad & m'_1 v = r'_1 \wedge \cdots \wedge m'_{k_1} v = r'_{k_1} \\ \wedge \quad & m''_1 v > r''_1 \wedge \cdots \wedge m''_{k_2} v > r''_{k_2} \end{aligned}$$

（ただし，m_j, m'_j, m''_jは正の自然数，r_j, r'_j, r''_jは変数vと演算記号$\cdot, /$を含まない項）の形であるとしてよい．$k_1 \geq 1$ならば，$k = 1, t_1 = r'_1/m'_1$ととればよい．$k_1 = 0, k_0 > 0, k_2 > 0$ならば，$\exists v \varphi(v)$ということは，$r_i/m_i$たちのうち最小のもの$r$よりも$r''_{i''}/m''_{i''}$たちのうち最大のもの$r''$のほうが小さいということと同値，これは$r'' < (r + r'')/2 < r$と同値だから，$\{k_n\}$として$(r_i/m_i + r''_{i''}/m''_{i''})/2$たちをとればよい．$k_0 = k_1 = 0, k_2 > 0$ならば，$r''_{i''}/m''_{i''}$たちのうち最大のもの$r''$より大きな$v$に対しては常に$\varphi(v)$が成立するから，$\{k_n\}$として$r''_{i''}/m''_{i''} + 1$たちをとればよい．同様に，$k_2 = k_1 = 0, k_0 > 0$ならば，$\{k_n\}$として$r_i/m_i - 1$たちをとればよい． □

RCOFの論理式φに演算記号$\cdot$が現れず，演算$/$の分母が常に$1 + \cdots + 1$の形ならば，各原子論理式の辺々に適当な自然数をかけることによってφは演算記号$\cdot, /$をもたない論理式と同値であることがわかる．このことと前の命題から次を得る．

命題 2.2.3. *1.* 量化記号と演算記号$\cdot, /$を持たない論理式$\varphi(\vec{v}, \vec{w})$に対し，変数$\vec{v}$たちを持たないAFの項の列の列$\mathbf{t}_1(\vec{w}), \mathbf{t}_2(\vec{w}), \ldots, \mathbf{t}_k(\vec{w})$で，

$$\mathsf{RCOF} \vdash [\exists \vec{v} \varphi(\vec{v}, \vec{w}) \leftrightarrow \varphi(\mathbf{t}_1(\vec{w}), \vec{w}) \vee \varphi(\mathbf{t}_2(\vec{w}), \vec{w}) \vee \cdots \vee \varphi(\mathbf{t}_k(\vec{w}), \vec{w})]$$

なるものが原始再帰的にとれる．
2. 演算記号$\cdot, /$を持たない論理式ψに対し，量化記号と演算記号$\cdot, /$を持たない論理式で，ψとRCOFにおいて同値なものがある． □

この命題から，SSCの部分的解決である次の定理を得る．

定理 2.2.4. 演算記号$\cdot, /$を持たない論理式φに対し，

$$\forall n [\mathrm{SAT}_{\mathbf{R}}(\exists v_{i_0} \exists v_{i_1} \cdots \exists v_{i_{n-1}} \varphi, E) \Rightarrow \exists A \in \mathbb{R}^n (\mathrm{SAT}_{\mathbf{R}}(\varphi, E^{i_0, i_1, \ldots, i_{n-1}}_{(A)_0, (A)_1, \ldots, (A)_{n-1}}))]$$

が成り立つ．

証明 前の命題の *2* により，φ は量化記号をもたないとしてよい．前の命題の *1* により，変数 $v_{i_0}, v_{i_1}, \ldots, v_{i_{n-1}}$ たちを持たない AF の項の列の列 $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ で，

$$\begin{aligned}\mathsf{RCOF} \vdash [\exists v_{i_0} \exists v_{i_1} \cdots \exists v_{i_{n-1}} \varphi(v_{i_0}, v_{i_1}, \ldots, v_{i_{n-1}}, \vec{w}) \\ \leftrightarrow \varphi(\mathbf{t}_1(\vec{w}), \vec{w}) \vee \varphi(\mathbf{t}_2(\vec{w}), \vec{w}) \vee \cdots \vee \varphi(\mathbf{t}_k(\vec{w}), \vec{w})]\end{aligned}$$

なるものが原始再帰的にとれる．$\mathrm{SAT}_{\mathbb{R}}(\exists v_{i_0} \exists v_{i_1} \cdots \exists v_{i_{n-1}} \varphi(v_{i_0}, v_{i_1}, \ldots, v_{i_{n-1}}, \vec{w}), E)$ が成り立つならば，$\mathrm{SAT}_{\mathbb{R}}(\varphi(\mathbf{t}_1(\vec{w}), \vec{w}) \vee \varphi(\mathbf{t}_2(\vec{w}), \vec{w}) \vee \cdots \vee \varphi(\mathbf{t}_k(\vec{w}), \vec{w}), E)$．したがって，ある $i \leq k$ に対し $\mathrm{SAT}_{\mathbb{R}}(\varphi(\mathbf{t}_i(\vec{w}), \vec{w}), E)$．このとき，定理 2.1.4 により，所要の有限実数列が $E, \mathbf{t}_i$ から得られる． □

この証明において，「この議論を n 回繰り返して…」などという強い帰納法を暗に用いるような議論を用いていないことに注意．未解決問題 SSC の難しさは，実数係数多項式 p の根たちをとり，それらを含む項を係数にもつ多項式の根たちをとり，再びそれらを含む項を係数にもつ多項式の根たちをとり … という操作を任意有限回繰り返すことで，それを RCA_0 で行う方法はまだ発見されていない．予想 2.2.1 を [6] と同じ方法で証明しようとすると，このような操作が本質的に必要になるのである．

なお，命題 2.2.2，命題 2.2.3，定理 2.2.4 の証明の複素数（ACF(0)）版も同様に（しかもより簡単に）証明できる．

2.3 代数学の基本定理

ここでは，代数学の基本定理が RCA_0 で証明できることを見る．既に，[8] において，RCA_0 で複素係数多項式の根の一つがとれることは示されているが，今回はより強い主張である，複素係数多項式の（重複を込めた）根全体の存在が RCA_0 で証明できることを見る．

定義 2.3.1. RCA_0 で次の定義をする．**有理複素数**とは，実部，虚部が共に有理数であるような複素数とする．これは有理数のペアでコード化される．有理複素数全体の集合を $\mathbb{E}$ で表す．$\mathbb{E}$ 係数多項式全体の集合を $\mathbb{E}[Z]$ で表す．特に，最高次の係数が 1 であるような 1 次以上の $\mathbb{E}$ 係数多項式全体の集合を $\mathbb{E}[Z]^*$ で表す．$\mathbb{E}[Z]$ の元は有理複素数有限列でコード化される．そして，$a_0 + a_1 Z + \cdots + a_{N-1} Z^{N-1} + a_N Z^N = P \in \mathbb{E}[Z]$ に対し，ノルムを $\|P\| = \max\{|a_0|, \ldots, |a_N|\}$ と定める．

次の定理の証明は [8] または [3] を参照のこと．

定理 2.3.2. RCA_0 で，

$$|P(\psi(P,n))| < 2^{-n}$$

を成り立たせる関数 $\psi : \mathbb{E}[Z]^* \times \mathbb{N} \to \mathbb{E}$ が存在する． □

$P \in \mathbb{E}[Z]^*, N = \deg P$ とする．このとき，$z \in \mathbb{E}$ が $|z| \geq 1 + N\|P\|$ を満たしていれば，

$$|P(z)| \geq |z|^N - N\|P\||z|^{N-1} = |z|^{N-1}(|z| - N\|P\|) > 1$$

となる．すなわち，上の定理で得られる関数 ψ は $|\psi(P,n)| < 1 + N\|P\|$ を成り立たせている．

これを用いて，$\varphi(P,n)$（$P \in \mathbb{E}[Z]^*, n \in \mathbb{N}$）を，$P$ の次数に関して再帰的に

$$\varphi(Z - z_0, n) = \langle z_0 \rangle,$$
$$N = \deg P > 1 \text{ のとき, } \varphi(P,n) = \langle \psi(P,t) \rangle^\frown \varphi(P',n)$$

（ここに，$t = 2^N \cdot n + 2$ で，$P'(Z)$ は $P(Z)$ を $(Z - \psi(P,t))$ で割った商，すなわち，$P(Z) = P(\psi(P,t)) + (Z - \psi(P,t))P'(Z)$）と定める．

命題 2.3.3. RCA_0 で，以下が示せる．任意の $P \in \mathbb{E}[Z]^*$，$z \in \mathbf{E}$ に対し，$|P(z)| < 2^{-2^{\deg P}\cdot(s+1)-1} \to \exists l < \deg P(|z - (\varphi(P,m))_l| < 2^{-s})$．

証明 $N = \deg P$ に関する Π^0_1-IND で証明する．$N = 1$ のときは $|P(z)| < 2^{-2^N\cdot(s+1)-1}$ ならば，$|(\varphi(P,m))_0 - z| < 2^{-2^N\cdot(s+1)-1} < 2^{-s}$ より成立．$N > 1$ の場合は，$t = 2^N \cdot s + 2, P(Z) = P(\psi(P,t)) + (Z - \psi(P,t))P'(Z)$ として，

$$\begin{aligned} |(z - \psi(P,t))P'(z)| \leq |P(z)| + |P(\psi(P,t))| &< 2^{-2^N\cdot(s+1)-1} + 2^{-t} \\ &< 2^{-2^N\cdot s}. \end{aligned}$$

従って，$|z - \psi(P,t)| \leq 2^{-2^N\cdot s-1} < 2^{-s}$ または $|P'(z)| \leq 2^{-2^N\cdot s-1} \leq 2^{-2^{(N-1)}\cdot(s+1)-1}$．後者の場合，帰納法の仮定によりある $l < N$ に対し，$|z - (\varphi(P',m))_l| < 2^{-s}$ だから，$|z - (\varphi(P,m))_{l+1}| < 2^{-s}$． □

$P \in \mathbb{E}[Z]^*$ に対し，$\widetilde{P}^n = (Z - (\psi(P,n))_0) \cdots (Z - (\psi(P,n))_{\deg P - 1})$ と定める．次の命題は，$\widetilde{P}^m$ が P の $\mathbb{E}$ で一次式に分解できる多項式による近似であることを表し

命題 2.3.4. RCA_0 で，以下が示せる．任意の $P \in \mathbb{E}[Z]^*$，$\deg P = N$, $m \in \mathbb{N}$ に対し，$\|P - \widetilde{P}^m\| < 2^{-2^N \cdot m + N - 1} \cdot (1 + \max\{|(\varphi(P,m))_0|, \ldots, |(\varphi(P,m))_{N-1}|\})^{N-1}$．特に，$\|P - \widetilde{P}^m\| < 2^{-2^N \cdot m + N - 1} \cdot (2 + N\|P\|)^{N-1}$.

証明 $N = \deg P$ に関する帰納法で示す．$N = 1$ の場合は $P = \widetilde{P}^m$ だから自明．$N > 1$ の場合，$t = 2^N \cdot m + 2, P(Z) = P(\psi(P,t)) + (Z - \psi(P,t))P'(Z)$ として，

$$\begin{aligned} P(Z) - \widetilde{P}^m(Z) &= P(\psi(P,t)) + (Z - \psi(P,t))P'(Z) - \widetilde{P}^m(Z) \\ &= P(\psi(P,t)) + (Z - \psi(P,t))(P'(Z) - \widetilde{P'}^m(Z)) \end{aligned}$$

だから，

$$\begin{aligned} & \|P(Z) - \widetilde{P}^m(Z)\| \\ \leq\ & (1 + |\psi(P,t)|)(1 + \max\{|(\varphi(P,m))_0|, \ldots, |(\varphi(P,m))_{N-1}|\})^{N-2} 2^{-2^{N-1} \cdot m + N - 2} \\ & + 2^{-t} \\ \leq\ & (1 + \max\{|(\varphi(P,m))_0|, \ldots, |(\varphi(P,m))_{N-1}|\})^{N-1} 2^{-2^{N-1} \cdot m + N - 1}. \end{aligned}$$

□

次の命題は [4] による．これは，多項式の係数を変化させるとき，多項式の根全体の変動は連続であることを表している．

命題 2.3.5. RCA_0 で，以下を満たす関数 $\nu : \mathbb{Q}_{>0} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ がとれる．$z_0, \ldots, z_{N-1}$, $w_0, \ldots, w_{N-1} \in \mathbb{E}$, $P(Z) = (Z - z_0) \cdots (Z - z_{N-1}), Q(Z) = (Z - w_0) \cdots (Z - w_{N-1})$ に対して，$\|P\| < R, \|Q\| < R, \|P - Q\| < 2^{-\nu(R,N,m)}$ となる $R \in \mathbb{Q}_{>0}$ が存在すれば，ある $0, 1, \ldots, N-1$ 上の置換 σ で，$|z_0 - w_{\sigma(0)}| < 2^{-m}, \ldots, |z_{N-1} - w_{\sigma(N-1)}| < 2^{-m}$ を満たすものがある．

証明 $H(R,N)$ を，$2^{H(R,N)} \geq (1 + NR)^N$ なる単調増加関数とし，$M(R,N)$ を，任意の $S \in \mathbb{E}[Z]$, $z, z' \in \mathbb{E}$ に対し，$\|S\| < 2^{H(R,N)} \wedge |z| < 2^{H(R,N)} \wedge |z'| < 2^{H(R,N)} \to |S(z) - S(z')| \leq 2^{M(R,N)}|z - z'|$ を成り立たせる単調増加関数とする．

$$\nu(R, 0, m) = m + H(R, 1)$$

$$\nu(R, N+1, m) = (N+1)(3\nu(R, N, m) + 2M(R, N) + (N+2)H(R, N+1) + 8)$$

ととればよい．これが所要の条件を満たすことを示すために，次のより強い主張を Σ^0_1-IND で示す．

$P(Z)=(Z-z_0)\cdots(Z-z_{N-1}), Q(Z)=(Z-w_0)\cdots(Z-w_{N-1})$ が任意の $|z|<2^{H(R,N)}$ なる $z\in\mathbb{E}$ に対し，$|P(z)-Q(z)|<(N+1)2^{NH(R,N)-\nu(R,N,m)}$ を成り立たせるならば，ある $0,1,\ldots,N-1$ 上の置換 σ で，$|z_0-w_{\sigma(0)}|<2^{-m},\ldots,|z_{N-1}-w_{\sigma(N-1)}|<2^{-m}$ を満たすものがある．

$N=1$ のとき，これが成り立つことは明らか．$N>1$ のとき，P,Q が任意の $|z|<2^{H(R,N)}$ なる $z\in\mathbb{E}$ に対し，$|P(z)-Q(z)|<(N+1)2^{NH(R,N)-\nu(R,N,m)}$ を成り立たせるならば，$|Q(z_0)|=|P(z_0)-Q(z_0)|<(N+1)2^{NH(R,N)-\nu(R,N,m)}<2^{NH(R,N)-\nu(R,N,m)+N}$．よって，ある i に対し，

$$\begin{aligned}|w_i-z_0| &\le 2^{(NH(R,N)-\nu(R,N,m))/N+1}\\ &= 2^{H(R,N)-(3\nu(R,N-1),m)+2M(R,N-1)+(N+1)H(R,N)+8)}\\ &= 2^{-3\nu(R,N-1,m)-2M(R,N-1)-NH(R,N)-8}\\ &< 2^{-m}.\end{aligned}$$

$i=n$ として一般性を失わない．$P^*(Z)=P(Z)/(Z-z_0), Q^*(Z)=Q(Z)/(Z-w_0)$ とおく．任意の $|z|<2^{H(R,N-1)}<2^{H(R,N)}, |z-z_0|>2^{-\nu(R,N-1,m)-M(R,N)-3}, |z-w_0|>2^{-\nu(R,N-1,m)-M(R,N)-3}$ なる $z\in\mathbb{E}$ に対し，

$$\begin{aligned}&|P^*(z)-Q^*(z)|\\ =\ &\left|\frac{P(z)(z-z_0)+P(z)(z_0-w_0)-Q(z)(z-z_0)}{(z-z_0)(z-w_0)}\right|\\ =\ &\frac{|P(z)-Q(z)|}{|z-w_0|}+\frac{|P(z)||z_0-w_0|}{|z-z_0||z-w_0|}\\ \le\ &|P(z)-Q(z)|2^{\nu(R,N-1,m)+M(R,N)+3}\\ &+|P(z)|2^{-3\nu(R,N-1,m)-2M(R,N-1)-NH(R,N)-8}\cdot(2^{\nu(R,N-1,m)+M(R,N)+3})^2\\ <\ &(N+1)2^{NH(R,N)-\nu(R,N,m)+\nu(R,N-1,m)+M(R,N)+3}\\ &+(N+1)2^{NH(R,N)-3\nu(R,N-1,m)-2M(R,N-1)-NH(R,N)-8+2\nu(R,N-1,m)+2M(R,N)+6}\\ <\ &(N+1)2^{-\nu(R,N-1,m)-2}+(N+1)2^{-\nu(R,N-1,m)-2}\\ <\ &(N+1)2^{-\nu(R,N-1,m)-1}\end{aligned}$$

が成り立つ．$w\in\mathbb{E}$ が $|w|<2^{H(R,N-1)}$ を成り立たせているとする．このとき，$z\in\mathbb{E}$ で，$|w-z|<2^{-M(R,N)-\nu(R,N-1,m)-2}$ と $|z|<2^{H(R,N-1)}<2^{H(R,N)}, |z-z_0|>$

$2^{-\nu(R,N-1,m)-M(R,N)-3}$,
$|z-w_0|>2^{-\nu(R,N-1,m)-M(R,N)-3}$ を満たすものがとれ，

$$\begin{aligned}
& |P^\star(w)-Q^\star(w)| \\
\leq\ & |P^\star(w)-P^\star(z)|+|P^\star(z)-Q^\star(z)|+|Q^\star(z)-Q^\star(w)| \\
\leq\ & 2^{M(R,N-1)+1}|z-w|+(N+1)2^{-N\nu(R,N-1,m)-1} \\
\leq\ & 2^{-\nu(R,N-1,m)-2+1}+(N+1)2^{-\nu(R,N-1,m)-1} \\
\leq\ & (N+1)2^{-\nu(R,N-1,m)} \\
\leq\ & N2^{(N-1)H(R,N-1)-\nu(R,N-1,m)}
\end{aligned}$$

となる．よって，帰納法の仮定により，$1,2,\ldots,N-1$ 上の置換 τ で，$|z_1-w_{\tau(1)}|<2^{-m},\ldots,|z_{N-1}-w_{\tau(N-1)}|<2^{-m}$ なるものがある．そこで，$\sigma(0)=0,\sigma(i)=\tau(i)(i>0)$ とすればよい． □

定理 2.3.6 (代数学の基本定理). RCA_0 で以下が示せる．任意の $A_0,\ldots,A_{N-1}\in\mathbb{C}$ に対し，

$$A_0+A_1Z+\cdots+A_{N-1}Z^{N-1}+Z^N=(Z-B_0)\cdots(Z-B_{N-1})$$

なる複素数列 $B_0,\ldots,B_{N-1}$ がとれる．

証明 各 A_i を，$\mathbb{E}$ の元の列 $a_{i,0},a_{i,1},\ldots$ で，$\forall j\forall k|a_{i,j}-a_{i,j+k}|<2^{-j}$ を満たすものとみる．このとき，$P_j=a_{0,j}+a_{1,j}Z+\cdots+a_{N-1,j}Z^{N-1}+Z^N$ とすれば，任意の j,k に対し $\|P_j-P_{j+k}\|<2^{-j}$．また，$R=\|P_0\|+1$ とすれば，任意の j に対し $\|P_j\|<R$．従って，

$$\begin{aligned}
\|\widetilde{P_j}^{\,j}-\widetilde{P_{j+k}}^{\,j+k}\| &\leq \|\widetilde{P_j}^{\,j}-P_j\|+\|P_j-P_{j+k}\|+\|P_{j+k}-\widetilde{P_{j+k}}^{\,j+k}\| \\
&< 2^{-2^N\cdot j+N-1}\cdot(2+N\|P_j\|) \\
&\quad +2^{-j}+2^{-2^N\cdot(j+k)+N-1}\cdot(2+N\|P_{j+k}\|) \\
&< 2^{-2^N\cdot j+N}\cdot(2+NR)+2^{-j} \\
&< 2^{-2^N\cdot j+N+1}\cdot(2+NR).
\end{aligned}$$

そこで，$\mathbb{E}$ の元の有限列の列 $\langle\langle b_{0,j},\ldots,b_{N-1,j}\rangle:j\in\mathbb{N}\rangle$ を，

$$b_{i,j}=(\varphi(P_{\nu(R,N,j)},\nu(R,N,j)))_i$$

ととり，各 $j > 0$ で $|b_{0,j} - b_{0,j-1}| + \cdots + |b_{N-1,j} - b_{N-1,j-1}|$ が最小になるように $b_{0,j}, \ldots, b_{N-1,j}$ を並べ替えれば，列 $B_i = \langle b_{i,0}, b_{i,1}, \ldots \rangle$ は所要の条件を満たす複素数を定める． □

3 帰納法，内包公理と実数

今までは RCA_0 で示すことができる実数に関する性質を見てきたが，ここではより強い公理を必要とする実数の性質を見る．また，RCA_0 により強い公理を加えることによる問題SSCの部分的解決をみる．

3.1 帰納法，内包公理と実数

$x \in \mathbb{R}$ が有理数であるという主張は

$$\exists q \in \mathbb{Q}(x = q)$$

と Σ^0_2 論理式で記述できる．この事実の発展として，次のこともわかる．

定理 3.1.1. RCA_0 で，以下の主張が同値なことが示せる．

1. Σ^0_2-BCA.

2. Σ^0_2-BCA を以下の形に制限したもの：

$$\forall l \forall n(\varphi(l,n) \leftrightarrow \psi(l,n)) \to \forall m \exists X(i \in X \leftrightarrow (i < m \wedge \exists x \forall y > x \varphi(i,y))$$

ここに，$\varphi \in \Sigma^0_1, \psi \in \Pi^0_1$ で，これらは X を自由変数として含まない．

3. 任意の $l \in \mathbb{N}$ について，長さ l の任意の実数列 A に対し，有限集合 B で

$$i \in B \leftrightarrow (i < l \wedge (A)_i \text{が有理数})$$

なるものが存在する．

証明 *1* $\to$ *3* は $(A)_i$ が有理数であるという主張が Σ^0_2 であることから直ちにわかる．

2 $\to$ *1*. $\varphi(x,y,i) \in \Sigma^0_0$ とする．$f, g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を次のように定める．

$$f(0,i) = g(0,i) = 0$$

$$\varphi(f(n,i), g(n,i), i) \Rightarrow [f(n+1,i) = f(n,i), g(n+1,i) = g(n,i) + 1]$$

$$\neg\varphi(f(n,i), g(n,i), i) \Rightarrow [f(n+1,i) = f(n,i) + 1, g(n+1,i) = 0]$$

このとき，関係 $g(y,i)\neq 0$ が Δ_1^0 だから，

$$\exists x\forall y\varphi(x,y,i)\leftrightarrow\exists x\forall y>x(g(y,i)\neq 0)$$

を示せば十分である．

まず $\rightarrow$ を示す．$\exists x\forall y\varphi(x,y,i)$ とする．Π_1^0-LNP により $\forall y\varphi(x,y,i)$ なる x のうち最小のものがとれる．すなわち，

$$\forall z<x\exists y\neg\varphi(z,y,i)\wedge\forall y\varphi(x,y,i)$$

このとき，任意の $j<x+1$ に対し，$f(l,i)=j\wedge g(l,i)=0$ なる l がとれることが Σ_1^0-IND によりいえる．特に $j=x$ として $f(l,i)=x\wedge g(l,i)=0$ なる l をとれば $\forall l'>l(g(l',i)\neq 0)$.

逆を示す．$\exists x\forall y>x(g(y,i)\neq 0)$ とすれば，Σ_1^0-IND（の対偶）により $\forall y(g(y,i)\neq 0)$ または $\exists x(g(x,i)=0\wedge\forall y>x(g(y,i)\neq 0))$ が成り立つ．$g(0,i)=0$ だから前者の場合は起こりえない．後者を成り立たせる x をとる．このとき，Σ_1^0-IND により，任意の $z\in\mathbb{N}$ に対し

$$f(x+z,i)=f(x,i)\wedge g(x+z,i)=z\wedge\varphi(f(x+z,i),g(x+z,i),i)$$

がいえる．$x'=f(x,i)$ とすれば，$\forall z\varphi(x',z,i)$.

$3\rightarrow 2$. $\varphi\in\Sigma_1^0,\psi\in\Pi_1^0$ が $\forall l\forall n(\varphi(l,n)\leftrightarrow\psi(l,n))$ を満たすとする．Δ_1^0 内包公理により $(x,i)\in X\leftrightarrow\varphi(x,i)$ なる X がとれる．有理数の2重列 $\langle q_{i,j}:i,j\in\mathbb{N}\rangle$ を

$$q_{i,0}=0$$

$$q_{i,j+1}=\begin{cases}q_{i,j} & (j,i)\in X\text{ のとき}\\ q_{i,j}+2^{-j^2-1} & (j,i)\notin X\text{ のとき}\end{cases}$$

で定める．$A_i=\langle q_{i,j}:j\in\mathbb{N}\rangle$ は実数になる．A_i は2進小数表示で，2^{-j^2-1} の位が，$\varphi(j,i)$ のとき，そしてそのときに限り0になり，その他の位は常に0になる実数を表す．このとき，

$$A_i\in\mathbb{Q}\leftrightarrow\exists x\forall y>x\varphi(y,i)$$

が成り立つことを示せば十分である．

$\leftarrow$ は明らかなので逆を示す．$\rightarrow$ の対偶を示す．$\forall x\exists y>x\neg\varphi(y,i)$ とする．任意の $n\in\mathbb{N}-\{0\}$ に対し $nA_i\notin\mathbb{Z}$ をいう．$2^k\leq n<2^{k+1}$ なる $k\in\mathbb{N}$ をとる．このとき，

$2^{k+1}A_i$ の小数部分 B は仮定 $\forall x\exists y > x\neg\varphi(y,i)$ より 0 でなく，$\langle q_{i,j}\rangle$ の定義により 2^{-2k} 未満である．すなわち $0 < B < 2^{-2k} \leq 1/n$．よって $2^{k+1}nA_i \notin \mathbb{Z}$．ゆえに $nA_i \notin \mathbb{Z}$．
□

無限個の実数に対する条件判定，計算を行おうとするとより強い公理が必要になる．

定理 3.1.2. RCA_0 で，以下の主張が同値なことが示せる．

1. ACA_0

2. Σ^0_1-CA

3. 任意の無限実数列 A に対し，集合 B で

$$i \in B \leftrightarrow ((A)_i = 0)$$

なるものが存在する．

4. 任意の無限実数列 A に対し，集合 B で

$$i \in B \leftrightarrow ((A)_i \text{は有理数})$$

なるものが存在する．

5. 任意の $E \in \mathbb{R}^{\mathbf{N}}$ に対し，無限実数列 $V_E = \langle V_E(s) : s \text{は RCOF の項のコード}\rangle$ で，定義 2.1.2 の V_E に関する条件を満たすものが存在する．

6. 任意の $E \in \mathbb{R}^{\mathbf{N}}$ に対し，集合 B で，

$$i \in B \leftrightarrow \mathrm{SAT}_{\mathbf{R}}(i, E)$$

なるものが存在する．

証明 *1* $\leftrightarrow$ *2* は [5] 参照．

1 $\rightarrow$ *6* は $\mathrm{SAT}_{\mathbf{R}}$ が Δ^0_2 なることからわかる．*1* $\rightarrow$ *5* も $V_E(t) = A$ が Δ^0_2 であることからわかる．*6* $\rightarrow$ *3* は自明であろう．

5 $\rightarrow$ *3*. $V_E(v_i/v_i) = \langle q^i_0, q^i_1, \ldots\rangle$ として，X を $i \in X \leftrightarrow q^i_2 < 1/2$ ととればよい．*3* $\rightarrow$ *2*. $\varphi \in \Sigma^0_0$ に対し，$f : \mathbb{N} \to \mathbb{N}$ を $f(i,j) = [\varphi(i,n)$ なる最小の $n < j$，ただしこのような $n < j$ が存在しないときは $j]$ と定める．そして，有理数の 2 重列 $\langle q_{i,j} : i,j \in \mathbb{N}\rangle$ を $q_{i,j} = 2^{-f(i,j)}$ で定める．$((A)_i)_j = q_{i,j}$ とすれば，A は実数の無限列で，$(A)_i \neq 0 \leftrightarrow \exists j\varphi(i,j)$ を満たす．よって，Y を $y \in Y \leftrightarrow (A)_y = 0$ ととり，X を $x \in X \leftrightarrow x \notin Y$ ととれば $x \in X \leftrightarrow \exists j\varphi(i,j)$．

$1 \to 4$ は $(A)_i$ が有理数であるという主張が Σ^0_2 であることからわかる．$4 \to 2$ は定理 3.1.1 の証明と同様にしてわかる． □

ここで，RCA_0 により強い公理を加えることによる SSC の部分的解決を試みよう．

定義 3.1.3 (有界従属選択公理). Γ を論理式の集合とする．公理図式 Γ-BDC を

$$\forall n \forall X \exists Y \varphi(n, X, Y) \to \forall l \exists Z \forall n < l \varphi(n, (Z)_n, (Z)_{n+1})$$

で定める．ここに，$\varphi \in \Gamma$ で，Z を自由変数として含まないものとする．

この公理図式は次の公理図式 Γ-BDC$'$

$$\forall n \forall X \exists Y \varphi(n, X, Y) \to \forall l \forall Z \exists W[(W)_0 = Z \wedge \forall n < l \varphi(n, (W)_n, (W)_{n+1})]$$

と RCA_0 上同値であること，並びに，任意の k に対し，$\mathsf{RCA}_0 + \Sigma^0_k$-BDC から Σ^0_k-IND が導出できること，$\mathsf{WKL}_0 + \Sigma^0_2$-IND から Σ^0_2-BDC が導出できることが知られている ([7] 参照)．

定理 3.1.4. 論理式 $\mathrm{SAT}_{\mathbb{R}}$ は次を満たすことが $\mathsf{RCA}_0 + \Sigma^0_2$-BDC で示せる：

$$\forall n[\mathrm{SAT}_{\mathbb{R}}(\exists v_{i+n-1} \exists v_{i+n-2} \cdots \exists v_i \varphi, E) \Rightarrow \exists A \in \mathbb{R}^n (\mathrm{SAT}_{\mathbb{R}}(\varphi, E^i_A))]$$

ここに，$E^i_A = E^{i,i+1,\ldots,i+n-1}_{(A)_0,(A)_1,\ldots,(A)_{n-1}}$ である．これから，

$$\forall n[\mathrm{SAT}_{\mathbb{R}}(\exists v_{i_0} \exists v_{i_1} \cdots \exists v_{i_{n-1}} \varphi, E) \Rightarrow \exists A \in \mathbb{R}^n (\mathrm{SAT}_{\mathbb{R}}(\varphi, E^{i_0,i_1,\ldots,i_{n-1}}_{(A)_0,(A)_1,\ldots,(A)_{n-1}}))]$$

もいえる．

証明 $\varphi(m, \gamma, i, F, F')$ を "$\mathrm{SAT}_{\mathbb{R}}(\exists v_{i+m} \exists v_{i+m-1} \cdots \exists v_i \gamma, F)$ ならば $[\forall j \neq i+m((F)_j = (F')_j)$ かつ $\mathrm{SAT}_{\mathbb{R}}(\exists v_{i+m-1} \exists v_{i+m-2} \cdots \exists v_i \gamma, F')]$ " を主張する Σ^0_2 論理式とする．このとき，各 m, i, γ, F に対し，$\mathrm{SAT}_{\mathbb{R}}(\exists v_{i+m} \exists v_{i+m-1} \cdots \exists v_i \gamma, F)$ ならば定理 2.1.4 により

$$\mathrm{SAT}_{\mathbb{R}}(\exists v_{i+m-1} \exists v_{i+m-2} \cdots \exists v_i \gamma, F^{i+m}_B)$$

なる実数 B がとれる．$F' = F^{i+m}_B$ とすれば $\forall j \neq i+m((F)_j = (F')_j)$ かつ $\mathrm{SAT}_{\mathbb{R}}(\exists v_{i+m-1} \exists v_{i+m-2} \cdots \exists v_i \gamma, F')$．よって $\forall m \forall F \exists F' \varphi(m, \gamma, i, F, F')$．ゆえに，$\Gamma$-BDC$'$ より $(W)_0 = E \wedge \forall m < n \varphi(m, \gamma, i, (W)_m, (W)_{m+1})$ なる W がとれる．$A \in \mathbb{R}^l$ を $(A)_j = ((W)_n)_{i+n-j}$ ととれば，Σ^0_2-IND により，任意の $l \in \mathbb{N}$ に対して

$$l < n+1 \to \mathrm{SAT}_{\mathbb{R}}(\exists v_{i+n-l-1} \exists v_{i+n-l-2} \cdots \exists v_i \gamma, E^i_{\langle (A)_0,(A)_1,\ldots,(A)_{l-1} \rangle})$$

がいえる．特に$l=n$として

$$\mathrm{SAT}_{\mathbf{R}}(\gamma, E^i_A)$$

を得る． □

この定理の複素数版も同様に示せる．

参考文献

[1] J. Barwise (ed.). *Handbook of Mathematical Logic.* Studies in Logic and the Foundations of Mathematics. North-Holland, 1977.

[2] P. G. Odifreddi. *Classical Recursion Theory.* Studies in Logic and the Foundations of Mathematics. North-Holland, 1989.

[3] P.C. Rosenbloom. An elementary constructive proof of the fundamental theorem of algebra. *American Mathematics Monthly*, Vol. 52, pp. 562–570, 1945.

[4] Wim B. G. Ruitenburg. Constructing roots of polynomials over the complex numbers. In *Computational Aspects of Lie Group Representations and Related Topics*, No. 84 in CWI Tract, 1991.

[5] S. G. Simpson. *Subsystems of Second Order Arithmetic.* Perspectives in Mathematical Logic. Springer-Verlag, 1999.

[6] K. Tanaka and T. Yamazaki. Manipulating the reals in RCA_0. Preprint.

[7] 田中一之, 山崎武. 2階算術と有界選択公理. 2階算術の諸体系の研究, 数理解析研究所講究録, No. 1096. 京都大学数理解析研究所, 1999.

[8] 齋藤晃. 2階算術における関数解析の基礎. 修士論文. 東北大学, 1996.